Complexity classes

Code: https://github.com/mesmere/sasha-tutorial/tree/main/tba-2

Decision problems

We care about problems with **yes/no answers**.

Not a decision problem:

Given a set S of integers, find a set $S' \subseteq S$ such that $\Sigma S'=0$.

Decision problem:

Is there *some* subset of S which sums to zero?

P and NP

P (polynomial) is the set of all decision problems with solutions that can be *found* in polynomial time.

NP (nondeterministic, polynomial) is the set of all decision problems with solutions that can be *verified* in polynomial time.

P = NP?

Reductions

A **reduction** from problem A to problem B is an algorithm which can solve problem A using an algorithm designed to solve problem B.

So you can think of it as an A-solving function which has two inputs: a function that can solve instances of problem B, and the instance of problem A to solve.

```
function solveInstanceOfA(funToSolveB, instanceOfA) { /* ??? */ }
```

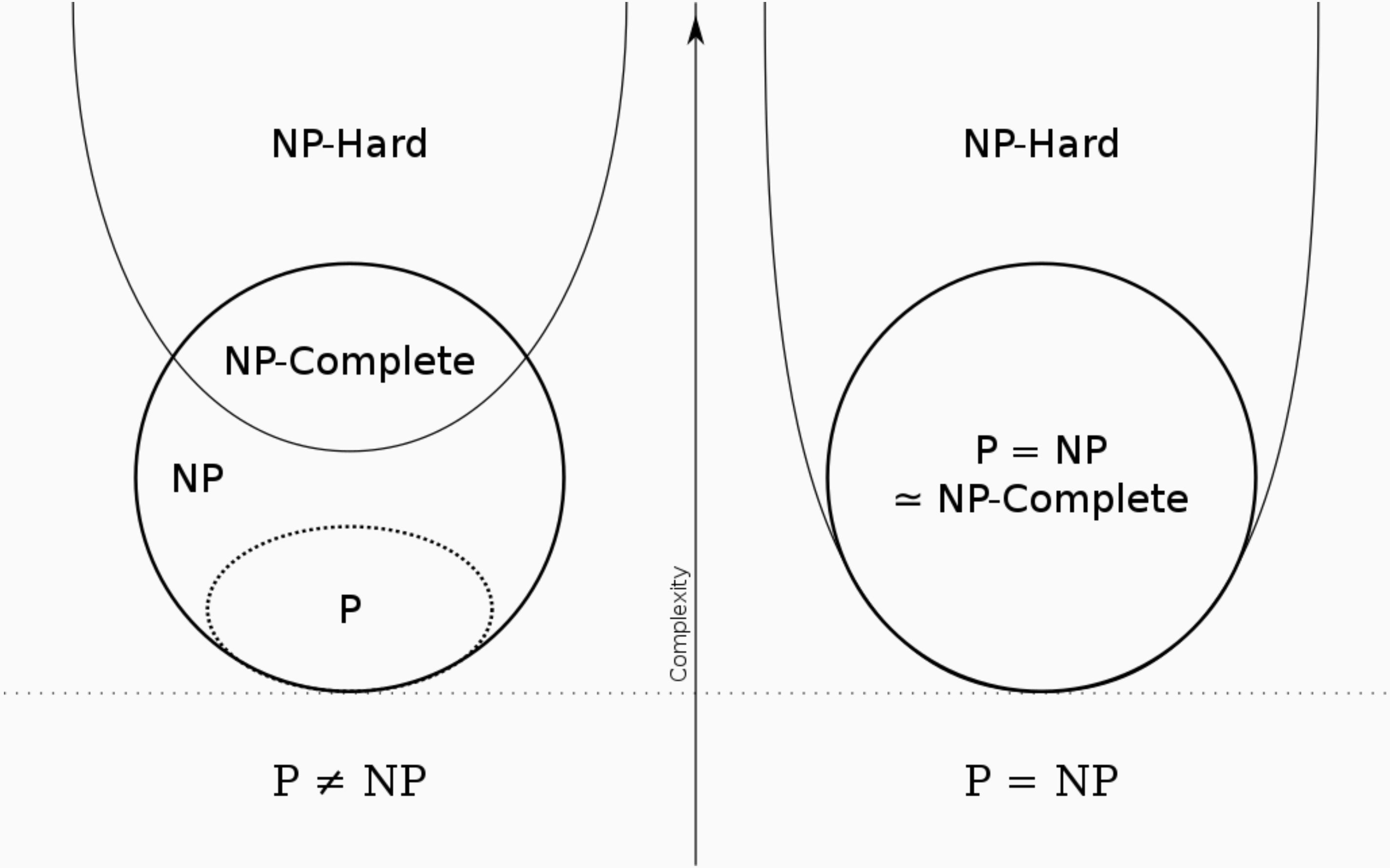
If such a reduction algorithm exists and it runs in polynomial time (except for calling `funToSolveB` at the end), we say that B is *polynomial-time m-reducible* to problem A.

NP-hardness

A decision problem is in **NP-hard** if there exists a polynomial-time reduction to it from every problem in NP.

A decision problem is **NP-complete** if it's in both NP *and* NP-hard.

Complexity classes



3-SAT

$$\exists \underbrace{A, B, C}_{\text{Any number of variables?}} : \underbrace{(A \vee \bar{B} \vee C)}_{\text{Exactly 3 terms per conjunct}} \wedge (\bar{A} \vee B \vee \neg C) \wedge (A \vee B \vee C) \wedge (\bar{A} \vee B \vee C)$$

ANDs between clauses

Each term may be inverted or not

Is this logical formula true? In other words, is the boolean expression inside the quantifier **satisfiable**?

Yes it is!

$(\bar{A}, B, C)$

CNF-SAT reduces to 3-SAT

CNF-SAT ("conjunctive normal form satisfiability") drops the requirement that there be exactly three terms per clause. E.g.:

$$\exists\, A, B, C, D : \underbrace{(A \lor \overline{B} \lor C \lor D)}_{\text{four terms}} \land \underbrace{(\overline{A} \lor B)}_{\text{two terms}}$$

We'll prove that there's a **polynomial-time m-reduction** from CNF-SAT to 3-SAT.

CNF-SAT reduces to 3-SAT

$$\exists A, B, C, D : (A \lor \overline{B} \lor C \lor D) \land (\overline{A} \lor B)$$

- Conjuncts with **too many terms** can be broken up:

$$\exists A, B, C, D : (A \lor \overline{B} \lor C \lor D)$$
$$\equiv \; \exists A, B, C, D, E : (A \lor \overline{B} \lor E) \land (C \lor D \lor \overline{E})$$

- Conjuncts with **too few terms** can be padded:

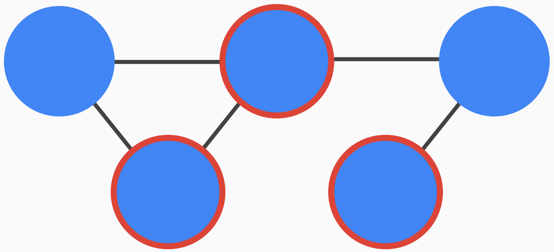
$$(\overline{A} \lor B) \equiv (\overline{A} \lor B \lor B)$$

Vertex cover

A **vertex cover** of a graph $G=(V, E)$ is a subset $V_C \subseteq V$ such that every edge in E is incident to at least one vertex in V_C.

The **minimum vertex cover problem** asks us to find a smallest-possible vertex cover given some graph.

The decision problem version asks us to determine whether a vertex cover exists with *at most k* vertices.

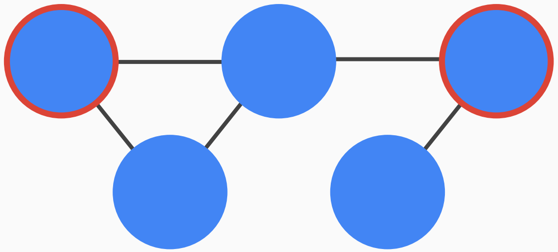


Independent set

An **independent set** of a graph G=(V, E) is a subset $V_I \subseteq V$ such that no two vertices in V_I are incident to the same edge.

The **maximum independent set** problem asks us to find a largest-possible independent set given some graph.

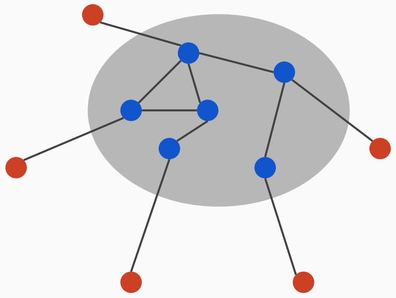
The decision problem version asks us to determine whether an independent set exists with *at least* k vertices.



VC reduces to IS, and IS reduces to VC

Insight: Given *any* vertex cover, the remaining vertices form an independent set!

In fact, a graph (V, E) has a vertex cover of size ≤ k iff the graph has an independent set of size ≥ |V| - k.



Arrange the vertices so that you can draw a circle around the vertex cover region.

Since there *can be* no edges between vertices outside, the remaining vertices form an independent set.

VC reduces to IS, and IS reduces to VC

VC $\leq_P$ IS : A graph (V, E) has a **vertex cover** of size $\leq k$ iff the graph has an **independent set** of size $\geq |V| - k$.

IS $\leq_P$ VC : A graph (V, E) has an **independent set** of size $\geq k$ iff the graph has a **vertex cover** of size $\leq |V| - k$.

So the vertex cover problem is *equivalent to* the independent set problem.

3-SAT reduces to IS

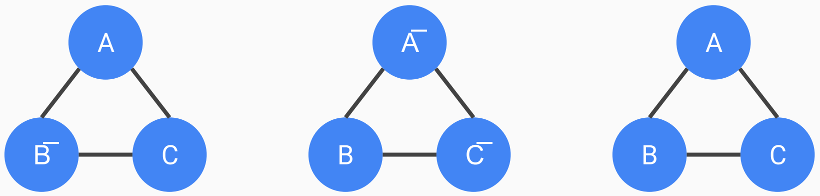
Given a 3-SAT problem:

$$(A \lor \bar{B} \lor C) \land (\bar{A} \lor B \lor \bar{C}) \land (A \lor B \lor C)$$

k=3
(number of clauses)

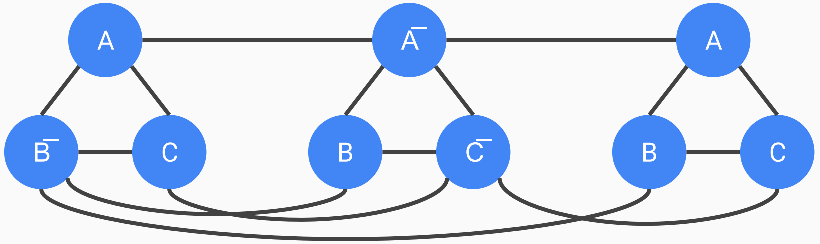
We can construct a corresponding “gadget” in polynomial time:

Step 1:



$O(k^2)$
expansion

Step 2:



The question “is there an independent set of size k=3 in this graph” answers the question of whether our original formula is satisfiable. 😎

IS and VC are in NP-complete

- We've just reduced 3-SAT to IS so we know that IS is in NP-hard.
- We can verify whether a purported IS solution is correct in polynomial time:
    - ✅ Check that the independent set has ≥k vertices.
    - ✅ Check that no edges have both ends in the independent set.

So IS is in NP-hard, and IS is in NP, therefore **IS is in NP-complete**.

Since the vertex cover problem is equivalent to the independent set problem, **vertex cover is in NP-complete too**.

Vertex cover approximation

"Clever" idea:

Repeatedly add the *highest-degree* vertex to our vertex cover, and remove it from the graph.

Off by a factor of lg n in the worst case!

"Dumb" idea:

Repeatedly pick a random edge and add *both* incident vertices to our vertex cover, then remove them from the graph.

Off by a factor of 2 in the worst case!

Other common NP-complete problems

- Does a given graph contain a Hamiltonian cycle? (Hamiltonian cycle problem)
- Does a given weighted graph contain a Hamiltonian cycle of length $\leq m$? (travelling salesperson problem)
- Does a given graph contain a complete subgraph of size k? (clique problem)
- Given two graphs G and H, is G a subgraph of H? (subgraph isomorphism problem)
- Can you color a given graph's vertices red, blue, and green such that no two vertices sharing an edge have the same color? (3-coloring problem)
- Given a multiset S of integers and a target T, is there some subset $S' \subseteq S$ such that $\Sigma S' = T$? (subset sum problem)
- Given disjoint sets X, Y, Z with $|X|=|Y|=|Z|$ and a set of triples ($x \ni X$, $y \ni Y$, $z \ni Z$) is there a subset of the triples which cover every element of X, Y, Z exactly once? (3-dimensional matching problem - but bipartite matching is in P...)
- Given an unbounded number of strings, do they all have a common subsequence of at least length n? (longest common subsequence problem)
- Minesweeper on an unbounded grid.

Minesweeper is NP-complete!

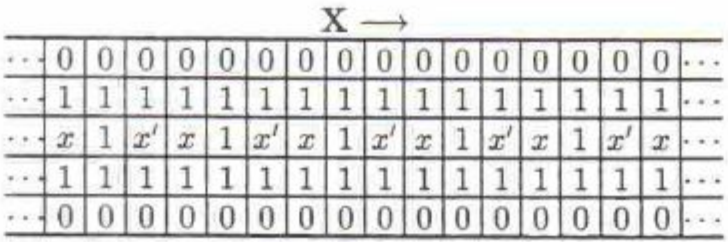


Figure 6. A wire.

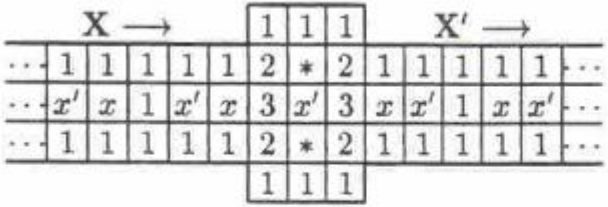


Figure 9. A NOT gate.

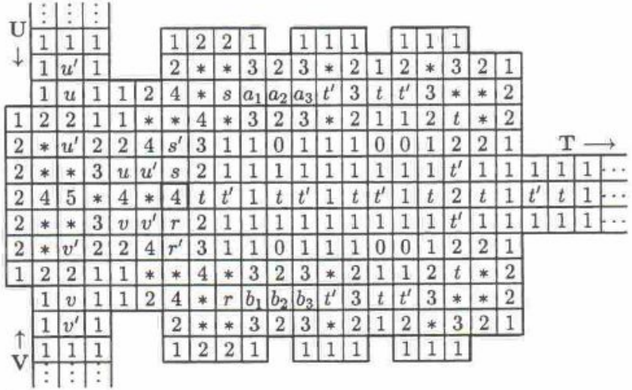


Figure 13. An AND gate.